培训大讲堂官方YY频道：3660

思科 **ASA** 和 **PIX** 防火墙配置手册

一、 配置基础..........2
- 1.1 用户接口..........2
- 1.2 防火墙许可介绍..........3
- 1.3 初始配置..........3

二、 配置连接性..........4
- 2.1 配置接口..........4
- 2.2 配置路由..........6
- 2.3 DHCP..........7
- 2.4 组播的支持..........7

三、 防火墙的管理..........7
- 3.1 使用 Security Context 建立虚拟防火墙（7.x 特性）..........7
- 3.2 管理 Flash 文件系统..........8
- 3.3 管理配置文件..........9
- 3.4 管理管理会话..........9
- 3.5 系统重启和崩溃..........10
- 3.6 SNMP 支持..........10

四、 用户管理..........11
- 4.1 一般用户管理..........11
- 4.2 本地数据库管理用户..........11
- 4.3 使用 AAA 服务器来管理用户..........11
- 4.4 配置 AAA 管理用户..........12
- 4.5 配置 AAA 支持用户 Cut-Through 代理..........12
- 4.6 密码恢复..........12

五、 防火墙的访问控制..........12
- 5.1 防火墙的透明模式..........12
- 5.2 防火墙的路由模式和地址翻译..........13
- 5.3 使用 ACL 进行访问控制..........15

六、 配置 Failover 增加可用性..........17
- 6.1 配置 Failover..........17
- 6.2 管理 Failover..........19

七、 配置负载均衡..........19
- 7.1 配置软件实现（只在 6500 native ios 模式下）..........19
- 7.2 配置硬件实现..........20
- 7.3 配置 CSS 实现..........22

八、 日志管理..........22
- 8.1 时钟管理..........22
- 8.2 日志配置..........23
- 8.3 日志消息输出的微调..........24
- 8.4 日志分析..........25

九、 防火墙工作状态验证..........25
- 9.1 防火墙健康检查..........25
- 9.2 流经防火墙数据的监控..........26

鸿鹄论坛：bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

9.3 验证防火墙的连接性......26
十、 Syslog 服务......28
Syslog 简介......28
Syslog 服务器的部署......29
10.1 内置 syslogd 的配置......29
10.2 配置基于 linux 的 syslog-ng 服务器......29
10.3 配置基于 Windows 的 syslog 服务器......30
10.4 路由器下 syslog 支持的配置......30
10.5 交换机下 syslog 支持的配置......31
10.6 PIX 防火墙下 syslog 支持的配置......32
10.7 VPN Concentrator 下 syslog 支持的配置......33
十一、 Cisco PIX 防火墙的问题集锦......33
11.1 如何允许外网用户 Telnet 至 PIX 的 outside？......33
11.2 我想通过在 pix 515e 上进行设置使某些内网用户只能上一个特定的网站......34
11.3 请教 pix515 acl 如何屏蔽一个网段？......35
11.4 在 515E 中配置 DHCP 网关的命令是什么......36
11.5 pix 能不能实现 dmz 和 inside 透明模式呢？......36
11.6 如何配置 PIX 透明模式?......37
11.7 为什么 ping 不通 515E 的 outside 地址？......37
11.8 pix515 的问题......40

一、 配置基础

1.1 用户接口

思科防火墙支持下列用户配置方式：

Console，Telnet，SSH（1.x 或者 2.0，2.0 为 7.x 新特性，PDM 的 http 方式（7.x 以后称为 ASDM）和 VMS 的 Firewall Management Center。

支持进入 Rom Monitor 模式，权限分为用户模式和特权模式，支持 Help，History 和命令输出的搜索和过滤。

注：Catalyst6500 的 FWSM 没有物理接口接入，通过下面 CLI 命令进入：

Switch# session slot slot processor 1 （FWSM 所在 slot 号）

用户模式：

鸿鹄论坛：bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

培训大讲堂官方YY频道：3660

Firewall> 为用户模式，输入 enable 进入特权模式 Firewall#。特权模式下可以进入配置模式，在 6.x 所有的配置都在一个全局模式下进行，7.x 以后改成和 IOS 类似的全局配置模式和相应的子模式。通过 exit，ctrl-z 退回上级模式。

配置特性：

在原有命令前加 no 可以取消该命令。Show running-config 或者 write terminal 显示当前配置，7.x 后可以对 show run 的命令输出进行搜索和过滤。Show running-config all 显示所有配置，包含缺省配置。Tab 可以用于命令补全，ctrl-l 可以用于重新显示输入的命令（适用于还没有输入完命令被系统输出打乱的情况），help 和 history 相同于 IOS 命令集。

Show 命令支持 begin，include，exclude，grep 加正则表达式的方式对输出进行过滤和搜索。

Terminal width 命令用于修改终端屏幕显示宽度，缺省为 80 个字符，pager 命令用于修改终端显示屏幕显示行数，缺省为 24 行，pager lines 0 命令什么效果可以自己试试。

1.2 防火墙许可介绍

防火墙具有下列几种许可形式，通过使用 show version 命令可以看设备所支持的特性：

Unrestricted (UR) 所有的限制仅限于设备自身的性能，也支持 Failover

Restricted (R) 防火墙的内存和允许使用的最多端口数有限制，不支持 Failover

Failover (FO) 不能单独使用的防火墙，只能用于 Failover

Failover-Active/Active (FO-AA) 只能和 UR 类型的防火墙一起使用，支持 active/active failover

注：FWSM 内置 UR 许可。

activation-key 命令用于升级设备的许可，该许可和设备的 serial number 有关（show version 输出可以看到），6.x 为 16 字节，7.x 为 20 字节。

1.3 初始配置

跟路由器一样可以使用 setup 进行对话式的基本配置。

鸿鹄论坛 bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

二、 配置连接性

2.1 配置接口

接口基础：

防火墙的接口都必须配置接口名称，接口 IP 地址和掩码（7.x 开始支持 IPv6）和安全等级。接口可以是物理接口也可以是逻辑接口（vlan），从 6.3 贾 C ?1t;/SPAN>trunk，但只支持 802.1Q 封装，不支持 DTP 协商。

接口基本配置：

注：对于 FWSM 所有的接口都为逻辑接口，名字也是 vlan 后面加上 vlanid。例如 FWSM 位于 6500 的第三槽，配置三个接口，分别属于 vlan 100,200,300.

Switch(config)# firewall vlan-group 1 100,200,300

Switch(config)# firewall module 3 vlan-group 1

Switch(config)# exit

Switch# session slot 3 processor 1

经过此配置后形成三个端口 vlan100.vlan200,vlan300

PIX 6.x

Firewall(config)# interface hardware-id [hardware-speed] [shutdown] （Hardware-id 可以用 show version 命令看到）

PIX 7.x

Firewall(config)# interface hardware-id

Firewall(config-if)# speed {auto | 10 | 100 | nonegotiate}

Firewall(config-if)# duplex {auto | full | half}

Firewall(config-if)# [no] shutdown

命名接口

FWSM 2.x

更多精彩IT资源敬请关注三通IT学院 www.santongit.com
鸿鹄论坛 bbs.hh010.com

Firewall(config)# nameif vlan-id if_name securitylevel

PIX 6.x

Firewall(config)# nameif {hardware-id | vlan-id} if_name securitylevel

PIX 7.x

Firewall(config)# interface hardware_id[.subinterface]

Firewall(config-if)# nameif if_name

Firewall(config-if)# security-level level

注：Pix 7.x 和 FWSM 2.x 开始支持不同接口有相同的 security level，前提是全局配置模式下使用 same-security-traffic permit inter-interface 命令。

配置 IP 地址

静态地址：Firewall(config)# ip address if_name ip_address [netmask]

动态地址：Firewall(config)# ip address outside dhcp [setroute] [retry retry_cnt]

注：setroute 参数可以同时获得来自 DHCP 服务器的缺省路由，再次输入此命令可以 renew 地址。

PPPOE：Firewall(config)# vpdn username JohnDoe password JDsecret

Firewall(config)# vpdn group ISP1 localname JohnDoe

Firewall(config)# vpdn group ISP1 ppp authentication chap

Firewall(config)# vpdn group ISP1 request dialout pppoe

Firewall(config)# ip address outside pppoe setroute

验证接口

Firewall# show ip

IPv6 地址配置（7.x 新特性）

暂略

ARP 配置

配置一个静态的 ARP 条目：Firewall(config)# arp if_name ip_address mac_address [alias]

鸿鹄论坛 bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

配置 timeout 时间：Firewall(config)# arp timeout seconds 缺省为 4 小时

注：一般情况下使用 clear arp 会清除所有的 ARP 缓存，不能针对单个的条目，但是可以通过以下变通方法：配置一个静态的条目，映射有问题的 ip 为一个假的 mac 地址，然后 no 掉该命令就会重新建立一个 arp 条目。

MTU 和分段

配置 MTU：Firewall(config)# mtu if_name bytes 使用 show mtu （6.3） 或者 show running-config mtu （7.x)来验证

分段（fragment）的几个命令：限制等待重组的分段数 Firewall(config)# fragment size database-limit [if_name]

限制每个包的分段数 Firewall(config)# fragment chain chain-limit [if_name]

限制一个数据包分段到达的时间 Firewall(config)# fragment timeout seconds [if_name]

配置接口的优先队列（7.x 新特性）

暂略

2.2 配置路由

启用 PRF 防止地址欺骗 Firewall(config)# ip verify reverse-path interface if_name

配置静态路由 Firewall(config)# route if_name ip_address netmask gateway_ip [metric]

配置 RIP

被动听 RIP 更新(v1，v2)Firewall(config)# rip if_name passive [version 1] （Firewall(config)# rip if_name passive version 2 [authentication [text | md5 key (key_id)]])

宣告该接口为缺省路由 Firewall(config)# rip if_name default version [1 | 2 [authentication [text | md5 key key_id]]

配置 OSPF

定义 OSPF 进程 Firewall(config)# router ospf pid

指定相应网络到 OSPF 区域 Firewall(config-router)# network ip_address netmask area area_id

可选：定义 Router ID Firewall(config-router)# router-id ip_address

记录 OSPF 邻居状态更新 Firewall(config-router)# log-adj-changes [detail]

更多精彩IT资源敬请关注三通IT学院 www.santongit.com

启用 OSPF 更新认证 Firewall(config-router)# area area_id authentication [message-digest] 宣告缺省路由 Firewall(config-router)# default-information originate [always] [metric value] [metric-type {1 | 2}] [route-map name]调节 OSPF 参数 Firewall(config-router)# timers {spf spf_delay spf_holdtime |lsa-group-pacing seconds}

2.3 DHCP

配置成为 DHCP Server：

配置地址池 Firewall(config)# dhcpd address ip1[-ip2] if_name （最多 256 个客户端）

配置 DHCP 参数 Firewall(config)# dhcpd dns dns1 [dns2] Firewall(config)# dhcpd wins wins1 [wins2] Firewall(config)# dhcpd domain domain_name Firewall(config)# dhcpd lease lease_length Firewall(config)# dhcpd ping_timeout timeout

启用 DHCP 服务 Firewall(config)# dhcpd enable if_name

验证：show dhcdp, show dhcpd bindings, show dhcpd statistics

配置 DHCP 中继：

定义真实 DHCP Server Firewall(config)# dhcprelay server dhcp_server_ip server_ifc(最多 4 个)

中继参数 Firewall(config)# dhcprelay timeout seconds Firewall(config)# dhcprelay setroute client_ifc

启用中继 Firewall(config)# dhcprelay enable client_ifc

验证 show dhcprelay statistics

2.4 组播的支持

暂略

三、 防火墙的管理

3.1 使用 Security Context 建立虚拟防火墙（7.x 特性）

特性介绍：从 PIX7.0 和 FWSM 2.2(1)开始，可以把物理的一个防火墙配置出多个虚拟的防火墙，每个防火墙称为 context，这样一个防火墙就支持两种工作模式：single-context 和 multiple-context，处

鸿鹄论坛 bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

于后者工作模式的防火墙被分为三个功能模块：system execution space(虽然没有 context 的功能，但是是所有的基础)，administrative context(被用来管理物理的防火墙) 和 user contexts(虚拟出来的防火墙，所有配置防火墙的命令都适用)

配置：首先使用 show activation-key 来验证是否有 multiple-context 的许可，然后通过 mode multiple 和 mode single 命令在这两个模式之间进行切换，当然也可以用 show mode 来验证现在工作在什么模式下。在不同 context 下进行切换使用 Firewall# changeto {system | context *name*}，由于所有的 context 的定义都必须在 system execution space 下，所以要首先使用 changeto system 转入该模式，Firewall(config)# context *name* 接着要把物理接口映射到 context 中 只要这样才能在相应的 context 下显示出物理接口，从而配置其属性 Firewall(config-ctx)# allocate-interface *physical-interface* [*map-name*] 最后定义 context 的 startup-config 的存放位置 Firewall(config-ctx)# config-url *url* 通过 show context 验证

注：当防火墙工作在 multiple-context 模式下，admin context 就自动生成。(show context 来验证)

由于所有的 context 都共享设备的资源，所以要限制各个 context 的资源分配

首先定义 class Firewall(config)# class *name* 然后 Firewall(config-class)# limit-resource all *number%* Firewall(config-class)# limit-resource [rate] *resource_name number[%]* 最后在相应的 context 配置下 Firewall(config-ctx)# member *class*

通过以下命令验证 show class， show resource allocation, show resource usage 等

注：缺省 telnet，ssh，IPsec 5 sessions，MAC address 65535 条目

3.2 管理 **Flash** 文件系统

6.x 文件系统

只有六种文件可以保存到 Flash，没有文件名只有代号，没有目录结构

0 OS 镜像 1 启动文件 2 VPN 和密匙证书 3 PDM 镜像 4 崩溃信息 5 0 的文件大小

show flashfs 显示 flash 文件

7.x 和 FWSM 文件系统

7.x 和 FWSM 更像 IOS 的文件系统，具有层级目录，要被格式化后才可以使用，7.x 使用 flash:/代表 Flash 文件系统，FWSM 分别使用 flash:/ (系统镜像)和 disk:/(配置文件)

由于该系统使用类 Unix 的指令，所以可以使用下列常用命令来对该文件系统操作：

dir pwd cd more delete copy rename mkdir rmdir format erase fsck(检查文件系统完整性)

更多精彩IT资源敬请关注三通IT学院 www.santongit.com
鸿鹄论坛 bbs.hh010.com

培训大讲堂官方YY频道：3660

6.x 在 Flash 里面只能保存一个系统镜像，7.x 则废除了此种限制通过使用 Firewall(config)# boot system flash:*filename* 来选取不同的系统镜像，show bootvar 进行验证

OS 升级 见附录

3.3 管理配置文件

7.0 以后可以使用多个启动配置文件 Firewall(config)# boot config *url*

显示启动配置文件 Firewall# show startup-config Firewall# show configuration (6.x 为 show configure)

保存当前配置文件 write memory, copy running-config startup-config, write net *[[server-ip-address]:[filename]]* (7.x 也支持 copy 至 tftp)

强制 standby 同步当前配置文件 write standby 删除启动配置文件 write erase

合并启动配置文件为当前配置文件 configure memory 从 Web 导入配置文件 configure http[s]://[user:password@]location[:port]/ http-pathname (7.x 支持 copy 自以上源)

合并配置文件自自动更新服务器

Firewall(config)# auto-update device-id {hardware-serial | hostname |

ipaddress [*if_name*] | mac-address *[if_name*] | string *text*}

Firewall(config)# auto-update server http[s]:/*/[username:password@]*

AUSserver-IP-address[:port]/autoupdate/AutoUpdateServlet

[verify-certificate]

3.4 管理管理会话

Firewall(config)# console timeout *minutes* 配置 console 登录的超时(缺省 0 不超时)

禁止来自 outside 端口的 telnet，启用 telnet Firewall(config)# telnet *ip_address netmask if_name* Firewall(config)# telnet timeout *minutes* 配置 telnet 超时

启用 SSH 配置

首先生成 RSA 密匙对 Firewall(config)# domain-name name Firewall(config)# ca generate rsa key [modulus] (7.x 使用 crypto key generate rsa general-keys [modulus modulus]) Firewall(config)# ca save all (7.x 自动保存)

鸿鹄论坛：bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

使用 show ca mypubkey rsa 来验证(7.x show crypto key mypubkey rsa) ca zeroize rsa 作废原有密匙对(7.x crypto key zeroize rsa default)

最后允许 ssh 会话 Firewall(config)# ssh ip_address netmask if_name

ssh version 命令可以选择 ssh 的版本，ssh timeout 定义超时时间

PDM/ASDM 配置

由于 PDM 存放位置固定，所以不需要指定镜像的位置，ASDM 使用 Firewall(config)# asdm image device:/path 来指定镜像位置，如果没有可以使用 copy 命令来安装。然后配置访问许可 Firewall# http ip_address subnet_mask if_name 启用 HTTP 进程 Firewall# http server enable 使用 https://ip-address/admin 来访问。

Banner 配置 Firewall(config)# banner {exec | login | motd} text 对 banner 不能修改，只能用 no 来删除，或者 clear banner 来清除所有的 banner（7.0 clear configure banner）

监控管理会话 who 监控 telnet 会话 kill telnet-id 来清除会话，show ssh sessions 监控 ssh 会话，ssh disconnect session-id 清除 ssh 会话，show pdm sessions 监控 pdm 会话，pdm disconnect session-id 清除 pdm 会话

3.5 系统重启和崩溃

通常使用 reload 命令重启系统，从 7.0 以后支持在特定的时间重启系统 Firewall# reload at hh:mm [month day | day month] [max-hold-time {minutes | hhh:mm}] [noconfirm] [quick] [save-config] [reason text]或者经过一定的时间间隔后重启 Firewall# reload in {minutes | hh:mm} [max-hold-time {minutes | hhh:mm}] [noconfirm] [quick] [save-config] [reason text]

启用崩溃信息生成 Firewall(config)# crashinfo save enable (7.0 no crashinfo save disable) show crashinfo 来看崩溃信息 clear crashinfo 删除信息（FWSM 使用 crashdump）

3.6 **SNMP** 支持

系统 SNMP 信息 Firewall(config)# snmp-server location string (contact string)

SNMP 访问许可 Firewall(config)# snmp-server host if_name ip_addr [poll | trap]

Firewall(config)# snmp-server community key

鸿鹄论坛 bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

四、 用户管理

4.1 一般用户管理

注：缺省情况下认证用户仅需要 password，这样的一般用户缺省用户名就是 enalbe_1,在 ssh 情况下缺省用户名就是 pix，然后用 password 来认证。

非特权模式密码配置 Firewall(config)# {password | passwd} password [encrypted] (恢复缺省密码 cisco 用 clear {password | passwd})

特权模式密码配置 Firewall(config)# enable password [pw] [level priv_level] [encrypted]

4.2 本地数据库管理用户

定义用户 Firewall(config)# username username [{nopassword | password password}

[encrypted]] privilege level

启用本地认证 Firewall(config)# aaa authentication {serial | telnet | ssh | http} console LOCAL

注：缺省情况特权模式密码使用 enable password 定义，这样用户通过认证后使用 enable 来进入特权模式，而不管用户初始什么等级的权限，所有用户使用相同的密码。这里也可以使用本地 enable 认证(aaa authentication enable console LOCAL)，用户使用 username password 的密码来进入 enable，用户 enable 密码独立从而增加安全性。

本地授权：Firewall(config)# aaa authorization command LOCAL

配置命令的特权等级：Firewall(config)# privilege {show | clear | configure} level level [mode {enable | configure}] command command

使用 show privilege 来看当前命令的特权等级(7.x 使用 show run all privilege)

4.3 使用 **AAA** 服务器来管理用户

定义 AAA 服务器组和协议 Firewall(config)# aaa-server server_tag protocol {tacacs+ | radius} (7.x 还增加了 kerberos,ldap,nt,sdi 协议的支持)

加入服务器到组 Firewall(config)# aaa-server server_tag [(if_name)] host server_ip [key] [timeout seconds]

可选命令

鸿鹄论坛 bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

定义服务器失败阀值 FWSM Firewall(config)# aaa-server server_tag max-attempts number

PIX 6.x Firewall(config)# aaa-server server_tag max-failed-attempts number

PIX 7.x Firewall(config-aaa-server-group)# max-failed-attempts number

定义统计策略(7.x 特性) Firewall(config-aaa-server-group)# accounting-mode {single | simultaneous}

具体各协议参数配置暂略

4.4 配置 **AAA** 管理用户

启用鉴权 Firewall(config)# aaa authentication {serial | telnet | ssh | http} console

server_tag [LOCAL]

启用授权 Firewall(config)# aaa authorization command server_tag [LOCAL]

启用统计 Firewall(config)# aaa accounting command [privilege level] server_tag

注：AAA 服务器配置略

4.5 配置 **AAA** 支持用户 **Cut-Through** 代理

4.6 密码恢复

五、 防火墙的访问控制

5.1 防火墙的透明模式

特性介绍：从 PIX 7.0 和 FWSM 2.2 开始防火墙可以支持透明的防火墙模式，接口不需要配置地址信息，工作在二层。只支持两个接口 inside 和 outside，当然可以配置一个管理接口，但是管理接口不能用于处理用户流量，在多 context 模式下不能复用物理端口。由于连接的是同一地址段的网络，所以不支持 NAT，虽然没有 IP 地址但是同样可以配置 ACL 来检查流量。

进入透明模式 Firewall(config)# firewall transparent (show firewall 来验证当前的工作模式，由于路由模式和透明模式工作方式不同，所以互相切换的时候会清除当前配置文件)

更多精彩IT资源敬请关注三通IT学院 www.santongit.com

培训大讲堂官方YY频道：3660

配置接口 Firewall(config)# interface hardware-id

Firewall(config-if)# speed {auto | 10 | 100 |nonegotiate}

Firewall(config-if)# duplex {auto | full | half}

Firewall(config-if)# [no] shutdown

Firewall(config-if)# nameif if_name

Firewall(config-if)# security-level level

注：不用配置 IP 地址信息，但是其它的属性还是要配置的，接口的安全等级一般要不一样，same-security-traffic permit inter-interface 命令可以免除此限制。

配置管理地址 Firewall(config)# ip address ip_address subnet_mask

Firewall(config)# route if_name foreign_network foreign_mask gateway [metric]

MAC 地址表的配置 Firewall# show mac-address-table 显示 MAC 地址表

Firewall(config)# mac-address-table aging-time minutes 设置 MAC 地址表过期时间

Firewall(config)# mac-address-table static if_name mac_address 设置静态 MAC 条目

Firewall(config)# mac-learn if_name disable 禁止特定接口地址学习(show mac-learn 验证)

ARP 检查 Firewall(config)# arp if_name ip_address mac_address 静态 ARP 条目

Firewall(config)# arp-inspection if_name enable [flood | no-flood] 端口启用 ARP 检查

为非 IP 协议配置转发策略 Firewall(config)# access-list acl_id ethertype {permit | deny} {any | bpdu | ipx | mpls-unicast | mpls-multicast | ethertype}

Firewall(config)# access-group acl_id {in | out} interface if_name

5.2 防火墙的路由模式和地址翻译

特性介绍：从高安全等级到低安全等级的访问称为 outbound 访问，需要配置地址翻译和 outbound 访问控制，PIX 缺省情况下不用配置 ACL 就允许此类访问，FWSM 则需要配置 ACL 来允许此类型的访问。而从低安全等级到高安全等级的访问称为 inboud 访问，也需要配置地址翻译和 inboud 访问控制，此类型必须配置 ACL.同一安全等级的访问也可以配置地址翻译。

支持下列几种 NAT 类型

更多精彩IT资源敬请关注三通IT学院 www.santongit.com

培训大讲堂官方YY频道：3660

Translation Type	**Application**	**Basic Command**	**Direction in Which Connections Can Be Initiated**
Static NAT	Real source addresses (and ports) are translated to mapped addresses (and ports)	static	Inbound or outbound
Policy NAT	Conditionally translates real source addresses (and ports) to mapped addresses	static access-list	Inbound or outbound
Identity NAT	No translation of real source addresses	nat 0	Outbound only
NAT exemption	No translation of real source addresses matched by the access list	nat 0 access-list	Inbound or outbound
Dynamic NAT	Translates real source addresses to a pool of mapped addresses	nat id global id address-range	Outbound only
PAT	Translates real source addresses to a single mapped address with dynamic port numbers	nat id global id address	Outbound only

配置

对于连接数的控制 PIX 6.x ... [norandomseq] [max_conns [emb_limit]]

PIX 7.x ... [norandomseq] [[tcp] max_conns [emb_limit]] [udp udp_max_conns]

连接超时控制 Firewall(config)# timeout [conn hh:mm:ss] [udp hh:mm:ss]

静态 NAT

基于地址的静态翻译 Firewall(config)# static (real_ifc,mapped_ifc) {mapped_ip | interface} {real_ip [netmask mask]} [dns] [norandomseq] [max_conns [emb_limit]]

基于端口的静态翻译 Firewall(config)# static (real_ifc,mapped_ifc) {tcp | udp} {mapped_ip | interface} mapped_port {real_ip real_port [netmask mask]} [dns] [norandomseq] [max_conns [emb_limit]]

策略 NAT

定义翻译策略 Firewall(config)# access-list acl_name permit ip real_ip real_mask foreign_ip foreign_mask

静态的 Firewall(config)# static (real_ifc,mapped_ifc) mapped_ip access-list acl_name [dns] [norandomseq] [max_conns [emb_limit]]

鸿鹄论坛 bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

NAT 的 Firewall(config)# global (mapped_ifc) nat_id {global_ip [-global_ip] [netmask global_mask]} | interface

Firewall(config)# nat (real_ifc) nat_id access-list acl_name [dns] [outside][norandomseq] [max_conns [emb_limit]]

Identify NAT Firewall(config)# nat (real_ifc) 0 real_ip real_mask [dns] [norandomseq] [max_conns [emb_limit]]

注：nat 0 和 static 相同地址的区别在于：nat 0 只能用于 outbound 访问，static 两种访问都可以，对同一地址不建议同时配置此两类命令。

NAT Exemption

Firewall(config)# access-list acl_name permit ip local_ip local_mask foreign_ip foreign_mask

Firewall(config)# nat (real_ifc) 0 access-list acl_name [dns] [outside] [max_conns [emb_limit] [norandomseq]]

注：此类型 NAT 策略只能根据源和目的地址不能根据协议类型或者端口

动态地址翻译

定义 NAT 的映射地址 Firewall(config)# global (mapped_ifc) nat_id global_ip[-global_ip] [netmask global_mask]

定义 PAT 的映射地址 Firewall(config)# global (mapped_ifc) nat_id {global_ip | interface}

定义翻译策略 Firewall(config)# nat (real_ifc) nat_id real_ip [mask [dns] [outside] [[norandomseq] [max_conns [emb_limit]]]

注：也可以使用 ACL 来做类似的策略 NAT。

5.3 使用 ACL 进行访问控制

特性介绍：防火墙的 ACL 配置跟 IOS 不同，子网掩码部分为正常的子网掩码不需要使用反转的子网掩码。还支持 Object group，包含 IP 地址组，ICMP 类型组，IP 协议或者端口组，并且支持组嵌套。access-list acl_name compiled 配置 Turbo ACL，7.x 自动 turbo。防火墙的 ACL 缺省是扩展模式的，7.x 后也支持标准模式了尽管只用于路由协议的配置上，并且加上了 extend 的参数，虽然配置的时候可以不必强制用这个参数但是当你需要移除该条目的时候要记得把 extend 这个参数加上。

配置

定义 Object Group

网络对象组 Firewall(config)# object-group network group_id

Firewall(config-network)# description text

Firewall(config-network)# network-object ip_addr mask (或者 host ip_addr)

Firewall(config-network)# group-object group_id

ICMP 对象组 Firewall(config)# object-group icmp-type group_id

Firewall(config-icmp-type)# description text

Firewall(config-icmp-type)# icmp-object icmp_type

Firewall(config-icmp-type)# group-object group_id

协议对象组 Firewall(config)# object-group protocol group_id

Firewall(config-protocol)# description text

Firewall(config-protocol)# protocol-object protocol

Firewall(config-protocol)# group-object group_id

服务对象组 Firewall(config)# object-group service group_id {tcp | udp | tcp-udp}

Firewall(config-service)# description text

Firewall(config-service)# port-object range begin_port end_port (或者 eq port)

Firewall(config-service)# group-object group_id

定义时间范围 7.0 特性

Firewall(config)# time-range name

Firewall(config-time-range)# periodic start-day hh:mm to end-day hh:mm

Firewall(config-time-range)# periodic days-of-the-week hh:mm to hh:mm

Firewall(config-time-range)# absolute [start hh:mm day month year] [end hh:mm day month year]

配置 ACL Firewall(config)# access-list acl_id [line line-num] [extended] {permit | deny}

{protocol | object-group protocol_obj_group} {source_addr source_mask | object-group network_obj_group} [operator sport | object-group service_obj_group]

更多精彩IT资源敬请关注三通IT学院 www.santongit.com

{destination_addr destination_mask |object-group network_obj_group}

[operator dport | object-group service_obj_group] [log [[disable | default] | [level]]] [interval secs]] [time-range name] [inactive]

show access-list 来验证， clear access-list acl_id counters 重置 ACL 计数器

六、 配置 Failover 增加可用性

特性介绍：为了增强可用性，避免单点故障，提高性能等原因才引入了 Failover 的特性。Active-Standby 是最初支持的一种特性，其中一台是 UR 的许可，另一台为 UR 或者 Failover-only 的许可，FWSM 缺省支持此中模式，在该模式下一个为 Active 工作状态，Standby 只是监控 Active 的状态而不工作，这样就在性能上虽然有两台设备但是并没有得到加强。在 7.x 以后由于引入了 context 的概念，这样 Active-Active 另一种 Failover 的特性也出现了，在每个 context 下有自己的 active 和 standby，配置每个设备在不同 context 下的角色从而使其都工作，也增加了性能，但是此模式只被 PIX515E，525,535 和 ASA 平台支持。

6.1 配置 Failover

确定主备用的设备：一种方式是通过不同的许可来决定，如果两者都是 UR 的许可，对于适用 serial 连接的根据线缆两端的主备用标识来决定，如果适用 lan 的话使用下面的命令来决定，

Firewall(config)# failover lan unit {primary | secondary}

配置 lan 使用的端口

FWSM 2.x Firewall(config)# failover interface ip if_name ip_address mask standby ip_address

PIX 6.x Firewall(config)# interface phy_if phy_speed

Firewall(config)# nameif phy_if if_name securitylevel

Firewall(config)# ip address if_name ip_address netmask

Firewall(config)# failover ip address if_name ip_address

PIX 7.x Firewall(config)# interface phy_if

Firewall(config-if)# speed speed

Firewall(config-if)# duplex duplex

Firewall(config-if)# no shutdown

Firewall(config-if)# exit

Firewall(config)# failover interface ip if_name ip_address mask standby ip_address

定义用于 Failover 通讯的接口

FWSM 2.x Firewall(config)# failover lan interface if_name vlan vlan

PIX 6.x   Firewall(config)# failover lan interface if_name

PIX 7.x   Firewall(config)# failover lan interface if_name phy_if

也可以使用 failover lan key key-string 命令对通讯进行加密

failover lan enable 启用 lan-based failover，FWSM 缺省使用此模式，不需要此命令。

对于 Active-Active 模式需要在主设备的 system execution space 下配置 Failover 组，

Firewall(config)# failover group {1 | 2}

Firewall(config-fover-group)# {primary | secondary}

Firewall(config-fover-group)# preempt

对接口使用虚拟的 MAC 地址

PIX 6.x Firewall(config)# failover mac address if_name active_mac standby_mac

PIX 7.x (A-S) Firewall(config)# failover mac address phy_if active_mac standby_mac

PIX 7.x (A-A)   Firewall(config)# failover group {1 | 2}

Firewall(config-fover-group)# mac address phy_if   active_mac standby_mac

定义健康监控策略

PIX 6.x Firewall(config)# failover poll time

PIX 7.x Firewall(config)# failover polltime [unit] [msec] time [holdtime holdtime]

Firewall(config)# failover polltime interface time

Firewall(config)# failover interface-policy num[%]

更多精彩IT资源敬请关注三通IT学院 www.santongit.com

Firewall(config)# monitor-interface if_name

保持 HTTP 的状态信息 Firewall(config)# failover replicate http

Firewall(config)# failover 启用 Failover 进程

6.2 管理 Failover

show failover 命令对状态进行监控，后面可以加 state,lan, history,等参数。

(no)Failover active 手动的对状态进行切换,重置一个失败的设备 failover reset。对于不能同步的挂起设备使用 failover reload-standby 强制重启。

七、 配置负载均衡

特性介绍：虽然使用 Failover 保证了高可用性，但是在流量分担上还有劣势，尽管 7.x 支持了 A-A 的模式，不过也仅仅只能是两台防火墙。真正的负载均衡的实现有三种方式，第一为软件方式，使用 6500 平台上 IOS SLB(Server Load Balancing)特性的一个子集 FWLB 来实现，第二为硬件方式，在 6500 上配置 CSM(Content Switching Module)来实现，最后一种为专属设备方式，思科的 CSS(Content Services Switch)产品线的设备来实现。要注意的是在配置负载均衡的时候要 inside 和 outside 同时配置，免得出现来回链路不同而被丢弃的情况。

7.1 配置软件实现 （只在 6500 native ios 模式下）

定义防火墙群的连接性 Router(config)# vlan vlan-id

Router(config)# interface vlan vlan-id

Router(config-if)# ip address ip-address subnet-mask

Router(config-if)# no shutdown

Router(config)# ip route inside-network subnet-mask fw-outside-address

定义针对每个防火墙失败的探测器 Router(config)# ip slb probe name ping

Router(config-slb-probe)# address ip-address

Router(config-slb-probe)# interval seconds

Router(config-slb-probe)# faildetect retry-count

鸿鹄论坛：bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

定义防火墙群 Router(config)# ip slb firewallfarm firewallfarm-name

Router(config-slb-fw)# real ip-address

Router(config-slb-fw-real)# probe probe-name

Router(config-slb-fw-real)# inservice

Router(config-slb-fw-real)# weight weighting-value

定义特定的数据流到该防火墙群(只针对 Outside)

Router(config-slb-fw)# access [source source-ip-address network-mask]

[destination destination-ip-address network-mask]

选择 FWLB 的方式 Router(config-slb-fw)# predictor hash address [port]

启用 FWLB Router(config-slb-fw)# inservice

7.2 配置硬件实现

进入 CSM 负载均衡模式 Switch(config)# ip slb mode csm

选择 CSM 模块 Switch(config)# module csm slot-number

配置到离开防火墙群的连接性 Switch(config-module-csm)# vlan vlan-id client

Switch(config-slb-vlan-client)# ip address ip-address netmask

Switch(config-slb-vlan-client)# gateway ip-address

Switch(config-slb-vlan-client)# exit

配置到防火墙群的连接性 Switch(config-module-csm)# vlan vlan-id server

Switch(config-slb-vlan-server)# ip address ip-address netmask

Switch(config-slb-vlan-server)# alias ip-address netmask

Switch(config-slb-vlan-server)# route ip-address netmask gateway gw-ip-address

定义防火墙探测器 Switch(config-module-csm)# probe probe-name icmp

Switch(config-slb-probe-icmp)# interval seconds

鸿鹄论坛：bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

Switch(config-slb-probe-icmp)# receive receive-timeout

Switch(config-slb-probe-icmp)# retries retry-count

Switch(config-slb-probe-icmp)# failed failed-interval

定义防火墙群 Switch(config-module-csm)# serverfarm serverfarm-name

Switch(config-slb-sfarm)# real ip-address

Switch(config-slb-real)# inservice

Switch(config-slb-sfarm)# predictor hash address {source | destination} 255.255.255.255

Switch(config-slb-sfarm)# no nat server

Switch(config-slb-sfarm)# probe probe-name

定义一个虚拟服务器来处理发往服务器群的流量

Switch(config-module-csm)# vserver virtual-server-name

Switch(config-slb-vserver)# serverfarm serverfarm-name

Switch(config-slb-vserver)# virtual ip-address [network-mask] any

Switch(config-slb-vserver)# vlan vlan-number

Switch(config-slb-vserver)# inservice

Switch(config-slb-vserver)# replicate csrp {sticky | connection}

定义一个通用服务器群处理离开防火墙群的流量

Switch(config-module-csm)# serverfarm serverfarm-name

Switch(config-slb-sfarm)# predictor forward

Switch(config-slb-sfarm)# no nat server

定义一个通用的虚拟服务器处理离开防火墙群的流量

Switch(config-module-csm)# vserver virtual-server-name

Switch(config-slb-vserver)# serverfarm serverfarm-name

Switch(config-slb-vserver)# virtual 0.0.0.0 0.0.0.0   any

更多精彩IT资源敬请关注三通IT学院 www.santongit.com

Switch(config-slb-vserver)# vlan vlan-number

Switch(config-slb-vserver)# inservice

7.3 配置 **CSS** 实现

配置 CSS 的物理接口 (config) interface interface_name

(config-if) bridge vlan vlan-id (或者(config-if) trunk)

指定 IP 地址 (config) circuit circuit_name

(config-circuit) ip address ip_address subnet_mask

(config-circuit-ip) enable

配置缺省路由 (config) ip route 0.0.0.0 0.0.0.0 next-hop-address

定义防火墙群的防火墙 (config) ip firewall index local_firewall_address remote_firewall_address remote_css_address

定义静态路由 (config) ip route ip_address subnet_mask firewall index distance

调整 Keeplive 时间 (config) ip firewall timeout seconds

验证命令 show ip firewall 防火墙状态，show ip routes firewall 到防火墙的静态路由，show flows 显示到防火墙的负载均衡连接。

八、 日志管理

8.1 时钟管理

定义时区 Firewall(config)# clock timezone zone-name hours [minutes]

定义夏令时 Firewall(config)# clock summer-time zone recurring [week weekday month

hh:mm week weekday month hh:mm] [offset]

Firewall(config)# clock summer-time zone date {day month | month day}

year hh:mm {day month | month day} year hh:mm [offset]

设置防火墙时钟 Firewall(config)# clock set hh:mm:ss {day month | month day} year

鸿鹄论坛 bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

时钟验证 Firewall# show clock [detail]

指定 NTP 服务器 Firewall(config)# ntp server ip-address [key number] [source if-name]

[prefer]

配置 NTP 认证 Firewall(config)# ntp authentication-key key-number md5 value

Firewall(config)# ntp trusted-key key-number

Firewall(config)# ntp authenticate

NTP 验证 show ntp, show ntp status, show ntp associations

8.2 日志配置

启用消息日志 Firewall(config)# logging on (7.x 用 logging enable)

使用事件列表定义日志策略 (7.0 特性)

Firewall(config)# logging list event_list level level [class event_class]

Firewall(config)# logging list event_list message start[-end]

根据不同日志级别定义目的位置 (7.0 特性)

Firewall(config)# logging class event_class destination level [destination level] [destination level] ...

发送日志到 console Firewall(config)# logging console level

发送日志到 telnet，ssh 会话 Firewall(config)# logging monitor level

发送日志到 buffer Firewall(config)# logging buffered level

发送日志到 ftp (7.0 特性) Firewall(config)# logging ftp-bufferwrap

Firewall(config)# logging ftp-server ftp_server path username password

发送日志到 flash (7.0 特性) Firewall(config)# logging flash-bufferwrap

Firewall(config)# logging flash-minimum-free kbytes_free

Firewall(config)# logging flash-maximum-allocation kbytes_max

发送日志到 SNMP 服务器 Firewall(config)# snmp-server host [if_name] ip_addr trap (7.x

更多精彩IT资源敬请关注三通IT学院 www.santongit.com

Firewall(config)# snmp-server host if_name ip_addr TRap [community string] [version version] [udp-port port])

Firewall(config)# snmp-server enable traps {all | syslog}

Firewall(config)# logging history level

发送日志到 Syslog 服务器 Firewall(config)# logging trap level

Firewall(config)# logging device-id {hostname | ipaddress if_name | string text}

Firewall(config)# logging host if_name ip_address [protocol/port] [format emblem]

Firewall(config)# logging timestamp

Firewall(config)# logging queue queue_size (show logging queue 验证)

Firewall(config)# logging facility facility

Firewall(config)# logging standby

发送日志到邮件 (7.x 特性) Firewall(config)# logging mail {level | event-list}

Firewall(config)# smtp-server server_primary [server_secondary]

Firewall(config)# logging from-address from_email_address

Firewall(config)# logging recipient-address to_email_address [level level]

发送日志到 ASDM Firewall(config)# logging asdm-buffer-size num_of_msgs

Firewall(config)# logging asdm {level | event-list}

验证 show logging

8.3 日志消息输出的微调

消息的修剪 Firewall(config)# no logging message message-number (show logging message 验证)

改变消息严重等级 Firewall(config)# logging message message-number [level level]

配置日志对 ACL 支持 Firewall(config)# access-list acl_name {permit | deny} ... log [level] [interval seconds]

Firewall(config)# access-list deny-flow-max n

更多精彩IT资源敬请关注三通IT学院 www.santongit.com
渡鸦论坛 bbs.the010.com

Firewall(config)# access-list alert-interval seconds

8.4 日志分析

对日志分析的软件

CS-MARS (http://www.cisco.com)

Network Intelligence Engine (http://www.network-intelligence.com)

Network Security Analyzer 和 FirewallAnalyzer Enterprise (http://www.eiqnetworks.com)

Sawmill Log Analyzer (http://www.sawmill.net)

CiscoWorks (http://www.cisco.com)

九、 防火墙工作状态验证

9.1 防火墙健康检查

CPU 负荷 Firewall# show cpu usage (show cpu usage context all 正常应该在 80%以下)

Show processes 显示防火墙当前活动进程，一般关注 Process 和 Runtime。

内存利用 Firewall# show memory

Xlate 表大小 Firewall# show xlate count

Conn 表大小 Firewall# show conn count

防火墙流量 使用 PDM，Syslog, show traffic 来计算或者 Perfmon 计数器 Firewall# show perfmon Firewall(config)# perfmon interval seconds ,perfmon {verbose | quiet}

Inspection 引擎和 Service Policy Firewall# show service-policy

Failover Firewall# show failover

端口状态 Firewall# show interface, 包队列状态 Firewall# show priority-queue statistics [if_name]

鸿鹄论坛 bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

9.2 流经防火墙数据的监控

特性介绍 对于流经防火墙数据的监控有两种方式 capture session 和 debug packet，两者区别在于前者可以后处理，多个进程，CPU 和内存利用率低，后者是实时显示，同时只能一个进程，且对资源利用率高，后者在 7.x 后已经不被支持。

配置 Capture

配置兴趣流量的 ACL Firewall(config)# access-list acl_id [line line-num] [extended] permit protocol {source_addr source_mask [operator sport] [destination_addr destination_mask [operator dport]]

配置 Capture Firewall# capture capture_name [access-list acl_name] [ethernet-type type]

[interface if-name] [buffer bytes] [circular-buffer] [packet-length bytes]

(7.x 支持 type {raw-data | isakmp | asp-drop drop-reason}参数)

show capture 显示当前的 Capture 会话， Firewall# show capture capture_name [access-list acl_name] [detail] [dump] 显示所抓包的信息。Firewall# copy capture:capture-name tftp://server/path [pcap] 拷贝信息至 TFTP， 如果启用 http 后可以用 https://firewall_address/capture/capture_name[/pcap]通过 Web 来显示或者下载。

clear capture capture_name 清空 capture 缓存但是保持会话， no capture capture_name interface if_name 停止 capture，从特定接口去除保持会话和缓存，no capture capture_name 彻底删除会话和缓存。

配置 Debug 模式 Firewall# debug packet if_name [src source_ip [netmask mask]] [dst dest_ip [netmask mask]] [[proto icmp] | [proto {tcp | udp} [sport src_port] [dport

dest_port]] [rx | tx | both]

9.3 验证防火墙的连接性

Ping 测试 Firewall# ping [if_name] host [data pattern] [repeat count] [size bytes] [timeout seconds] [validate]

ARP 缓存检查 show arp

路由表检查 show route

Traceroute 测试 traceroute 命令前提配置 Firewall(config)# access-list acl_name permit icmp any any eq echo

Firewall(config)# access-list acl_name permit icmp any any eq echo-reply

更多精彩IT资源敬请关注三通IT学院 www.santongit.com

Firewall(config)# access-list acl_name permit icmp any any eq unreachable

Firewall(config)# access-list acl_name permit icmp any any eq time-exceeded

Firewall(config)# access-list acl_name permit udp any range 32768 65535 any range 33434 33523

Firewall(config)# access-list acl_name permit udp any dns_address eq domain (可选)

ACL 检查 show access-group, show access-list

NAT 验证 Firewall# show xlate [detail] [global | local ip1[-ip2] [netmask mask]] lport | gport port[-port]] [interface if1[,if2][,ifn]] [state static [,dump] [,portmap] [,norandomseq] [,identity]] [debug] [count]

Firewall# show xlate [{global | local} ip1[-ip2] [netmask mask]] [{lport | gport} port[-port]] [interface if1[,if2][,ifn]] [state {static | portmap | identity | norandomseq}] [debug] [detail]

Firewall# show conn [state state_type] [{foreign | local} ip1[-ip2] netmask mask] [long] [{lport | fport} port1[-port2]] [protocol {tcp | udp}]

监控特定主机 Firewall# show local-host [ip_address] [all] [detail]

Firewall# clear xlate global global_ip [netmask mask] [gport global_port]

Firewall# clear xlate local local_ip [netmask mask] [lport local_port]

Firewall# clear xlate interface if_name_1[,if_name_2]

Firewall# clear xlate

超时参数 Firewall(config)# timeout xlate hh[:mm[:ss]]

Firewall(config)# timeout conn hh[:mm[:ss]]

Firewall(config)# half-closed hh[:mm[:ss]]

Firewall(config)# udp hh[:mm[:ss]]

Shun 检查 show shun， show shun statistics

鸿鹄论坛 bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

培训大讲堂官方YY频道：3660

用户认证检查 show uauth show url-server stats

配置更新检查 启用 AAA 记录用户命令记录

十、 Syslog 服务

讲述 Syslog 的架构和如何在思科的网络环境下部署 Linux 和 Win 下的 syslog 服务器,以及相应思科设备的配置.

Syslog 简介

Syslog 协议允许设备向消息收集器发送相应的事件信息.使用 UDP 端口 514,不需要确认,大小为 1024 字节.包含 Facility,Severity,Hostname,Timestamp,Message 五种信息.

Facility 是 syslog 对信息源的大致分类,比如该事件来源于操作系统,进程等,用整数表示.其中 16-17 的 local use 可以为哪些没有被明确定义的进程或者应用所使用,通常思科 IOS 设备,CatOS 交换机,VPN3000 使用 Facility Local7 发送 syslog 信息,PIX 防火墙使用 local4,当然这些缺省值是可以修改的.

Severity 信息源或者 Facility 根据信息的严重程度使用 1 位数字进行分类.

数字	严重程度
0	Emergency: 报告软件或者硬件问题
1	Alert
2	Critical
3	Error
4	Warning
5	Notice: 系统重启或者接口 up.down
6	Informational
7	Debug: Debug 命令的输出

Hostname 设备名或者 IP 地址,如果多接口使用传送信息端口的 IP 地址.

Timestamp 时间戳是本地时间,IOS 允许添加时区信息,前面加个特殊字符比如*,格式如下: MMM DD HH:MM:SS Timezone *.

Message 信息.

鸿鹄论坛：bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

培训大讲堂官方YY频道：3660

Syslog 服务器的部署

10.1 内置 **syslogd** 的配置

/etc/syslog.conf 文件控制 syslogd 的配置.里面有根据 facility 和 severity 来定义的规则,格式为 facility.severity<Tab>destination-file-path,里面缺省的记录系统的信息不需要更改.对于思科设备来说 facility 从 local0 到 local7,severity 为前面提到的 debug,info,notice,warning,err,crit,alert,emerg 和 none.为了方便定义规则文件有下列特殊字符的定义:

字符	功能
,	在一句话定义相同 seveity 级别的多个 facilities,例如 local1,local5.debug
;	分开多个 facility.severity 语句在一条规则,常和!选项合用
*	指定所有的 facilities 或者 severities.
None	给定的 facility 没有 severity
=	指定某个 facility 下特定的 severity 比如 local7.=debug 只记录 level7 信息在 debug 级别而不包含剩下的 info, notice, warning 等信息,缺省会包含下级的 severity 信息
!	忽略特定的 severity 的级别,包含下级的.格式为 facility.!severity. 比如 local7.*;local7.!err 记录所有的 local7 信息但是忽略 severity 等级为 error, critical, alert 和 emergency 的信息.
@	定义远端的 syslog 服务器地址.格式为 facility.severity<Tab>@hostname. 如果使用主机名确保主机名在/etc/hosts 文件中已经加入

一个复杂的例子如下:

local6.*;local6.!=err /var/log/allexcepterror.log 写入所有 facility 为 local6 的信息到 all*.log 文件,只排除 severity 为 err 的信息

缺省情况下 syslogd 只能接收来自本地的 syslog 信息,如果要接收远端的 syslog 信息,启动的时候要加上-r 选项

10.2 配置基于 **linux** 的 **syslog-ng** 服务器

由于内置 syslogd 的有 facility 分类笼统,信息过滤弱等缺陷,推荐使用 syslog-ng 来替代.去该网站下载安装后通过修改/etc/syslog-ng 文件来进行软件的配置.该文件包含 5 个部分:options,source,destination,filter 和 log.

Options 定义全局选项,格式为 options { option1(value); option2(value); ... };

Source 定义守护进程收集信息的源,格式为 source identifier { source-driver(params); source-driver(params); ... };

更多精彩IT资源敬请关注三通IT学院 www.santongit.com

Destination 定义所收集信息经过过滤后保存的地方,格式为 destination identifier { destination-driver(params); destination-driver(params);

例子 destination hosts { file("/var/log/host/$DATE" create_dirs(yes)); }; 按照日期来保存文件,如果没有相应的目录为自动创建.

Filter 定义过滤规则,格式为 filter identifier { expression; };

Log 把 source,filter,destination 合并,实现来自某个 source 的信息符合特定的 filter 后送到所定义的 destination.格式为 log { source(s1); source(s2); ...filter(f1); filter(f2); ...destination(d1); destination(d2); ...flags(flag1[, flag2...]); };

10.3 配置基于 **Windows** 的 **syslog** 服务器

Kiwi Syslog 是一个免费的图形化 syslog 服务软件,安装配置比较简单.

配置思科设备对 syslog 的支持

10.4 路由器下 **syslog** 支持的配置

配置示例:

Router(config)#logging 192.168.0.30　　　配置 syslog 服务器地址,可以定义多个

Router(config)#service timestamps debug datetime localtime show-timezone msec

Router(config)#service timestamps log datetime localtime show-timezone msec　syslog 信息包含时间戳

Router(config)#logging facility local3　定义 facility 级别,缺省为 local7,可以设置从 local0 到 local7

Router(config)#logging trap warning　定义 severity 级别缺省为 infor 级别

Router(config)#end

Router#show logging

Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)

Console logging: level debugging, 79 messages logged

Monitor logging: level debugging, 0 messages logged

Buffer logging: disabled

Trap logging: level warnings, 80 message lines logged

Logging to 192.168.0.30, 57 message lines logged

10.5 交换机下 **syslog** 支持的配置

配置示例:

Console> (enable) set logging timestamp enable 定义信息包含日期戳

Console> (enable) set logging server 192.168.0.30 指定服务器地址,最多可以指定 3 个

Console> (enable) set logging server facility local4 定义 facility 级别,缺省为 local7,

Console> (enable) set logging server severity 4 定义 severity 级别除了前面提到的路由器上的 severity 级别以外还有一些交换机特有的

Console> (enable) set logging server enable 启用 syslog 服务

Console> (enable) show logging

Logging buffered size: 500

timestamp option: enabled

Logging history size: 1

Logging console: enabled

Logging server: enabled

{192.168.0.30}

server facility: LOCAL4

server severity: warnings(4

Current Logging Session: enabled

Facility	Default Severity	Current Session Severity
-------------	-----------------------	------------------------
cdp	3	4

鸿鹄论坛 bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

drip	2	4

10.6 **PIX** 防火墙下 **syslog** 支持的配置

配置示例:

Firewall(config)# loggin timestamp 定义信息包含日期戳

Firewall(config)# logging host 192.168.0.30 服务器地址,可以指定以 udp 或者 tcp 来发送信息,对于思科的 PIX FW syslog 软件只发送 tcp.

Firewall(config)# logging facility 21 定义 facility 级别,防火墙使用两位字符,local0 对应 16,依次类推,缺省为 20 也就是 local4

Firewall(config)# logging trap 7 定义 severity 级别,7 为 debug,0 为 emer,1 为 alert.

Firewall(config)# logging on 启用 syslog

Firewall(config)# no logging message 111005 抑制特定的 syslog 信息

Firewall(config)# exit

Firewall# show logging

Syslog logging: enabled

    Facility: 21

    Timestamp logging: enabled

    Standby logging: disabled

    Console logging: disabled

    Monitor logging: disabled

    Buffer logging: disabled

    Trap logging: level debugging, 6 messages logged

        Logging to inside 192.168.0.30

    History logging: disabled

    Device ID: disabled

更多精彩IT资源敬请关注三通IT学院 www.santongit.com

10.7 **VPN Concentrator** 下 **syslog** 支持的配置

在 web 管理界面下 Configuration > System > Events > Syslog Servers 通过 add 来增加 syslog server 的地址和 facility 级别. Configuration > System > Events > General 下通过 severity to syslog 的下拉菜单选择发送信息的 serverity 级别.然后保存修改.

neoshi@gmail.com

十一、 **Cisco PIX** 防火墙的问题集锦

11.1 如何允许外网用户 **Telnet** 至 **PIX** 的 **outside**？

补充一下
Licensed Features:
VPN-DES: Enabled
VPN-3DES: Disabled

用 SSH 就可以。 telnet 不可以！

对 inside 倒 dmz 的访问，需要做 nat 配 CRIPT language=javascript src="/CMS/JS/newsad.js">
置，对于 dmz 到 inside 的访问，需要做 static 与 access-list 的配置。

PIX 515E 连接 ADSL 路由 MODEM！

想知道 E0 口上怎么配置与开启路由的 MODEM 的连接。让内网所有用户可以都通过这个 MODEM 上网。
ADSL MODEM IP:192.168.1.1
pixfirwall(config)#vpdn group <组名> request dialout pppoe
pixfirwall(config)#vpdn group <组名> ppp auth PAP/CHAP/MSCHAP
pixfirwall(config)#vpdn group <组名> localname <拨号的用户名>
pixfirwall(config)#vpdn username <用户名> password <密码>
pixfirwall(config)#ip add <接口名称－随便定义> pppoe

鸿鹄论坛：bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

培训大讲堂官方YY频道：3660

11.2 我想通过在 **pix 515e** 上进行设置使某些内网用户只能上一个特定的网站

当前配置如下:

PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100

hostname pixfirewall
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
pager lines 24
mtu outside 1500
mtu inside 1500
ip address outside 61.155.88.82 255.255.255.252
ip address inside 10.10.3.253 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 3 interface
nat (inside) 3 10.10.1.1 255.255.255.255 0 0
nat (inside) 3 10.10.1.9 255.255.255.255 0 0
nat (inside) 3 10.10.1.81 255.255.255.255 0 0
nat (inside) 3 10.10.1.82 255.255.255.255 0 0
nat (inside) 3 10.10.1.113 255.255.255.255 0 0
nat (inside) 3 10.10.1.161 255.255.255.255 0 0

鸿鹄论坛 bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

nat (inside) 3 10.10.1.162 255.255.255.255 0 0
nat (inside) 3 10.10.1.165 255.255.255.255 0 0
nat (inside) 3 10.10.1.240 255.255.255.255 0 0
nat (inside) 3 10.10.2.240 255.255.255.248 0 0
nat (inside) 3 10.10.1.240 255.255.255.240 0 0
route outside 0.0.0.0 0.0.0.0 61.155.88.81 1
route inside 10.0.0.0 255.0.0.0 10.10.3.254 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc

0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media

0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:72a261056ba18f4dbefab375fb871688
: end

是的，可以将针对这些主机的限制策略放在 acl 的最上端，应用在 inside 口的 in 的方向上。

你可以用支持时间的 acl 来做，也可以用 tacacs 来验证用户，定义 downloaded acl

11.3 请教 **pix515 acl** 如何屏蔽一个网段？

deny ip host 61.129.64.* any
61.129.64.*这样的网段该咋样屏蔽？

更多精彩IT资源敬请关注三通IT学院 www.santongit.com

juechen70 (版主)
deny ip 61.129.64.0 255.255.255.0

csco10334975 (普通用户)
deny ip 61.129.64.0 255.255.255.0 any

mythis (普通用户)
access-list 100 deny ip 61.129.64.0 255.255.255.0 any

pix 上启用了 DHCP，不允许内网自动获取只允许 DMZ 自动获如何做。

dhcpd address 192.118.0.5-192.118.0.254 dmz
dhcpd enable dmz
dhcpd dns 219.141.136.10 218.247.141.68
这样就可以了！

pix7.0 如何在 routed 和 transparent 两种方式中切换?
我的 pix 515e 升级到 pix7.01 我想使用 transparent 模式， 请大家教如何做了？

firewall transparent
no firewall transparent

11.4 在 **515E** 中配置 **DHCP** 网关的命令是什么

dhcpd enable inside

11.5 **pix** 能不能实现 **dmz** 和 **inside** 透明模式呢？

有客户想把服务器搬到 dmz 区，但是服务器地址不变，这样除了透明模式我还想不到其他办法，inside 和 outside 的透明模式我知道，但是

inside 和 dmz 的透明模式怎么办？地址必须改变。透明桥模式下是没有 DMZ 概念的。地址不变也可以.做地址映射的时候翻译相同的地址就行了. 但是想搬到 dmz 区的机器和 inside 区的机器是同一网段的服务器和用户都是用一网段的，不改变地址怎么搞？

鸿鹄论坛：bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

11.6 如何配置 **PIX** 透明模式**?**

首先，需要升级 pix os 到 7.0.1
直接输入 firewall transparent 命令就可以让 PIX 工作在透明模式下面。 工作在透明模式下时，pix 相当于一条网线，故障切换由其它的三层设

备完成。
做防火墙的策略一般多是和端口对应的,外网在透明模式时怎样访问内网 HTTI.HTTPS.PPTP,TCP/UDP-5060/1270

有一点，透明模式下必须设置管理地址才会通
有所变化，以前用ＰＩＸ５１５双机作ｆａｉｌｏｖｅｒ，pix os 版本好像是６．３就不支持透明模式．看来透明模式的应用还是挺多的，可以做网络分区之间的安全隔离，最重要的是可以让动态路由协议穿过．

如何看用命令看这两台 PIX 支持的最大连接数（不是使用中的最大连接数，而是 license 所限制的最大连接数）
show ver.

11.7 为什么 **ping** 不通 **515E** 的 **outside** 地址？

PIX 的版本是 6.3(4)，设置了 515E 的 outside 地址和 inside 地址后，用网线将笔记本和 515E 的 outside 端口联起来，本本的地址和 outside 地址在

一个网段内，但总是 ping 不通 outside 地址，但同样的配置在 6.2 版本的 515E 上使用时是没有问题的，好奇怪啊？？

icmp pemit any outside

==

pix vpn 设置好了，DDN 方式可以上，为什么家里的 adsl 不行？

配置如下：pix520

PIX Version 6.3(3)
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full

鸿鹄论坛：bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

```
nameif ethernet0 Outside security0
nameif ethernet1 inside security100
nameif ethernet2 Outside-DMZ security50
enable password GyBjREM5Y/fIjrzB encrypted
passwd enO4Olec9w1AmAwd encrypted
hostname PIX-yinhetech
domain-name test.cn
clock timezone CST 8
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol ftp 2121
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
no fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
name 10.128.1.0 notebookpoolIP
access-list nonat permit ip 10.10.0.0 255.255.0.0 notebookpoolIP 255.255.255.0
access-list 101 permit ip 10.10.0.0 255.255.0.0 any
access-list notebookpc_splitTunnelAcl permit ip 10.10.0.0 255.255.0.0 any
access-list notebookpc_splitTunnelAcl permit ip notebookpoolIP 255.255.255.0 any
access-list notebookpc_splitTunnelAcl permit ip host 10.6.4.11 any
access-list Outside_cryptomap_dyn_20 permit ip any notebookpoolIP 255.255.255.0
access-list Outside_cryptomap_dyn_20 permit ip notebookpoolIP 255.255.255.0 any
pager lines 24
logging on
logging standby
logging buffered debugging
logging trap notifications
icmp deny any Outside
mtu Outside 1500
mtu inside 1500
mtu Outside-DMZ 1500
ip address Outside ***.***.***.** 255.255.255.240
ip address inside 10.127.1.253 255.255.255.0
ip address Outside-DMZ 172.18.3.254 255.255.255.0
ip verify reverse-path interface Outside
```

鸿鹄论坛：bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

```
ip verify reverse-path interface inside
ip audit info action alarm
ip audit attack action alarm
ip local pool notebookpool 10.128.1.1-10.128.1.250
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address Outside
no failover ip address inside
no failover ip address Outside-DMZ
pdm history enable
arp timeout 14400
global (Outside) 1 ***.***.***.** netmask 255.255.255.240
global (Outside-DMZ) 1 172.18.3.200-172.18.3.250 netmask 255.255.255.0
nat (inside) 0 access-list nonat
nat (inside) 1 10.0.0.0 255.128.0.0 0 0
access-group 101 in interface inside
route Outside 0.0.0.0 0.0.0.0 ***.***.***.** 1
route inside 10.0.0.0 255.128.0.0 10.127.1.254 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
http server enable
http 10.10.10.74 255.255.255.255 inside
http 10.10.10.88 255.255.255.255 inside
snmp-server host inside 10.10.10.10
snmp-server host inside 10.10.10.74
snmp-server location soft_yuan_internet
snmp-server contact bill
snmp-server community public
snmp-server enable traps
tftp-server inside 10.10.10.74 /
no floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto dynamic-map Outside_dyn_map 20 match address Outside_cryptomap_dyn_20
crypto dynamic-map Outside_dyn_map 20 set transform-set ESP-DES-MD5
crypto map Outside_map 65535 ipsec-isakmp dynamic Outside_dyn_map
crypto map Outside_map interface Outside
isakmp enable Outside
```

鸿鹄论坛 bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

培训大讲堂官方YY频道：3660

isakmp identity address
isakmp keepalive 60 5
isakmp nat-traversal 120
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash md5
isakmp policy 20 group 2
isakmp policy 20 lifetime 86400
vpngroup notebookpc address-pool notebookpool
vpngroup notebookpc dns-server 10.10.10.68 202.103.224.68
vpngroup notebookpc default-domain yhgroup.cn
vpngroup notebookpc split-tunnel notebookpc_splitTunnelAcl
vpngroup notebookpc idle-time 1800
vpngroup notebookpc password ********
telnet 10.0.0.0 255.128.0.0 inside
telnet 10.10.10.110 255.255.255.255 inside
telnet 10.10.10.110 255.255.255.255 Outside-DMZ
telnet timeout 31
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:826ec1728f5df3bb3ecf0542790a4d35

surf_qj (普通用户)

对了，是使用 cisco system VPN Client 4.01 登录的，家里 adsl 可以连上 VPN，但是不能访问，DDN 就可以其实，不光是 PIX 问题，我用 2620 做的和你的也一样，用一般的 ADSL 是不行的，但如果是用带路由功能 ADSL 就可以。

isakmp nat-traversal 120
还有客户端 NAT 打开，估计是 NAT 穿透的问题吧。

==

11.8 **pix515** 的问题

具体现象是，DMZ 和 inside 各接一台单机，DMZ 的单机能用上网，其他不能，inside 的机器什么都干不了。单机保证无问题。请各位帮忙看看配置吧。 outside 的地址和 global 的地址不同，有影响么？（没有空闲的连续地址了,只能用两个不同地址表示一下）
PIX Version 6.2(2)

鸿鹄论坛 bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
enable password O53fPNRgHkA6IEsY encrypted
passwd TWjtI1emvjruV4SY encrypted
hostname jygatewall
domain-name 219.2.2.2
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sqlnet 1521
fixup protocol sip 5060
no fixup protocol skinny 2000
no fixup protocol smtp 25
names
access-list dmz_jygate_acl deny icmp any any
access-list dmz_jygate_acl permit udp any any eq domain
access-list dmz_jygate_acl permit tcp any any eq www
access-list dmz_jygate_acl permit udp any any eq 20
access-list dmz_jygate_acl permit tcp any host 219.150.1.1 eq 20817
access-list dmz_jygate_acl permit tcp any host 219.150.1..1eq 20820
access-list dmz_jygate_acl permit tcp any host 219.150.1.1 eq 8080
access-list dmz_jygate_acl permit tcp any host 219.150.1.1 eq 8383
access-list dmz_jygate_acl permit tcp any host 219.150.1.1 eq 32002
pager lines 24
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full
mtu outside 1500
mtu inside 1500
mtu dmz 1500
ip address outside 219.150.1.2 255.255.255.224
ip address inside 192.168.168.1 255.255.255.0
ip address dmz 172.172.172.1 255.255.0.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
```

鸿鹄论坛 bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

培训大讲堂官方YY频道：3660

failover ip address inside 0.0.0.0
failover ip address dmz 0.0.0.0
pdm history enable
arp timeout 14400
global (outside) 1 219.150.1.2
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (dmz,outside) 219.150.1.2 172.172.172.101 netmask 255.255.255.255 0 0

static (inside,dmz) 192.168.168.0 192.168.168.0 netmask 255.255.255.0 0 0
access-group dmz_jygate_acl in interface outside
access-group dmz_jygate_acl in interface dmz
route outside 0.0.0.0 0.0.0.0 219.150.1.3 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 si
p 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt security fragguard
no sysopt route dnat
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:594b9bbf77abf8a342afee1764e4f7cd
: end

nyb0319 (普通用户)

no static (inside,dmz) 192.168.168.0 192.168.168.0 netmask 255.255.255.0 0 0
改为 static (inside,dmz) 172.172.172.1 192.168.168.0 netmask 255.255.255.0 0 0

加一条

static (inside,outside)
219.150.1.2 192.168.168.0
netmask 255.255.255.0 0 0

鸿鹄论坛 bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com

培训大讲堂官方YY频道：3660

no access-group dmz_jygate_acl in interface dmz

crazytank (普通用户)

按照上面的提示改了，结果提示 global address overlaps with mask 请各位大侠再帮忙看看啊

lcschina (活跃用户) ip address outside 219.150.1.2 255.255.255.224

global (outside) 1 219.150.1.2

地址重叠!!!

加上 global (outside) 1 interface 去掉你的那个 global

鸿鹄论坛 bbs.hh010.com
更多精彩IT资源敬请关注三通IT学院 www.santongit.com